REMARKS

Claims 1-13 are currently pending. Claims 9, 10, and 12 have been amended for clarification. In claim 10, a subscript has been added after the recitation of the received ciphertext C on line 5. It is respectfully submitted that no new matter has been added.

The Patent Office noted that information disclosure statements must be accompanied by each cited foreign patent document and non-patent literature publication or relevant portion. It is noted that the information disclosure statement of 2002 listed three non-patent literature articles – all of which have been initialed by the examiner as having been considered. In any event, appended hereto are further copies of the three referred publications.

The Patent Office objected to the drawings as failing to comply with 37 CFR 1.84(p)(5) because the part number 1 of Figure 1 is not mentioned in the description. The first line of the paragraph from page 6, line 36, through page 7, line 14, has been amended to designate part number 1 as the cryptographic system. This is supported by line 1 of original claims 1, 5, 8, and 11. It is respectfully submitted that no new matter has been added and respectfully requested that the Patent Office withdraw its objection to the drawings.

The Patent Office objected to the abstract as having more than 150 words. The abstract has been amended to have 150 or fewer words and is presented on a separate sheet. It is respectfully submitted that no new matter has been added and respectfully requested that the Patent Office withdraw its objection to the Abstract.

The Patent Office objected to the disclosure because two terms – DES and IDEA – have not been defined. Since the replacement paragraph for the paragraph on page 1, lines 29-35, has expanded DES as "Data Encryption Standard" and the replacement paragraph from page 7, line 16, through page 8, line 1, has expanded IDEA as "International Data Encryption Algorithm," as is known in the prior art, it is respectfully submitted that no new matter has been added and respectfully requested that the Patent Office withdraw its objection to the disclosure because of informalities.

The Patent Office rejected claim 9 under 35 U.S.C. 112, Second Paragraph, because the limitation "switching to one of said second cryptographic algorithms" lacks antecedent basis. The term "said second cryptographic algorithms" has been replaced with - - a plurality of second cryptographic algorithms - - for clarification. It is respectfully submitted that no new matter has been added and respectfully requested that the Patent Office withdraw its rejection of claim 9 under 35 U.S.C. 112, Second Paragraph.

The Patent Office rejected claim 12 under 35 U.S.C. 112, Second Paragraph, because the limitation "computer software product as claim 10" lacks antecedent basis. The dependency of claim 12 has been changed from "claim 10" to - - claim 11 - - for clarification. Claim 12 has also been amended to clarify the term "said at least one second cryptographic algorithms." It is respectfully submitted that no new matter has been added and respectfully requested that the Patent Office withdraw its rejection of claim 12 under 35 U.S.C. 112, Second Paragraph.

Claim 1 recites

> A cryptographic system (1) comprising
>
> first cryptographic algorithm means (2) for enabling cryptographic operations, input/output means (3, 4) for receiving input streams and sending output streams wherein said input streams are transformed to said output streams by said cryptographic operations,
>
> at least one test plaintext P_i and for each test plaintext P_i a corresponding test ciphertext C_i,
>
> receiving means (5) for receiving a control stream which is including at least one apoptosis key K_i ,
>
> **checking means (6) for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i,**
>
> switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm means (2), wherein said stopping by said switching means (7) is triggered by said checking means (6).

Claim 5 recites

> A method for creating a cryptographic system (1) for carrying out cryptographic operations characterized by the steps of
>
> implementing within said cryptographic system (1) a first cryptographic algorithm enabling said cryptographic operations,
>
> **selecting at least one test plaintext P_i and enciphering each test**

plaintext P_i with said first cryptographic algorithm and with a corresponding apoptosis key K_i thereby generating a corresponding test ciphertext C_i for each test plaintext P_i ,

implementing within said cryptographic system (1) said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i

implementing within said cryptographic system (1) receiving means (5) for receiving a control stream which is including at least one apoptosis key K_i ,

implementing within said cryptographic system (1) checking means (6) for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i,

implementing within said cryptographic system (1) switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm, wherein said stopping by said switching means (7) is triggered by said checking means (6).

Claim 8 recites

A method for operating a cryptographic system (1) for carrying out cryptographic

operations characterized by the steps of

providing a first cryptographic algorithm for enabling said cryptographic operations, receiving input streams and sending output streams wherein said input streams are transformed to said output streams by said cryptographic operations,

receiving a control stream which is including at least one apoptosis key K_i,

checking whether a test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i,

stopping said cryptographic operations with said first cryptographic algorithm, if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i.

Claim 11 recites

A computer software product for operating a cryptographic system (1) for carrying out cryptographic operations, said product is characterized by a computer-readable medium in which program instructions are stored, which instructions, when read by a computer, enable the computer to

perform a first cryptographic algorithm that is enabling said cryptographic operations,

receive input streams and send output streams wherein said input streams are transformed to said output streams by said cryptographic operations,

receive a control stream which is including at least one apoptosis key K_i ,

check whether a test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i,

stop said cryptographic operations with said first cryptographic algorithm, if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i.

The present invention concerns plaintext, ciphertext test pairs and is directed to a method for detecting compromise of cryptographic operations because the ciphertext generated by a first cryptographic algorithm from a test plaintext indicates that an apoptosis key has been used (page 4, lines 3-5 and 24-27). Upon detection of an apoptosis key by the generation of ciphertext corresponding to that apoptosis key encrypting the designated plaintext, cryptographic algorithms should be switched (page 4, lines 27-35). An advantage of the solution of the present invention is "that there is no need for controlling respectively trusting the manufacturer or a security service" (page 5, lines 11-12).

The Patent Office rejected claims 1, 3, 5, 7, 8, 10, 11, and 13 under 35 U.S.C. 103(a) as being unpatentable over Kocher et al. (US Patent Number 6,327,661) and further in view of Tschudin (NPL Apoptosis – the Programmed Death of Distributed Services).

The Patent Office asserted that Kocher discloses "checking means for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (column 13, lines 20-67)."

Specifically, claim 1 recites "checking means (6) for **checking whether said at least one**

test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i, switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm means (2), wherein said stopping by said switching means (7) is triggered by said checking means (6).”

Claim 5 recites “**selecting at least one test plaintext P_i and enciphering each test plaintext P_i with said first cryptographic algorithm and with a corresponding apoptosis key K_i thereby generating a corresponding test ciphertext C_i for each test plaintext P_i**, implementing within said cryptographic system (1) said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext $C_{i,}$ implementing within said cryptographic system (1) receiving means (5) for receiving a control stream which is including at least one apoptosis key K_i , **implementing within said cryptographic system (1) checking means (6) for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i**, implementing within said cryptographic system (1) switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm, wherein said stopping by said switching means (7) is triggered by said checking means (6).

Claim 8 recites “**checking whether a test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i**, stopping said cryptographic operations with said first cryptographic algorithm, if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i. ”

Claim 11 recites “**check whether a test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i**, stop said cryptographic operations with said first cryptographic algorithm, if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i.

In the claimed invention, if the test ciphertext corresponds to the test plaintext that results from the apoptosis key, the first cryptographic algorithm is stopped.

Kocher does not disclose checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i . Furthermore, Kocher does not disclose test plaintext, test ciphertext pairs. Instead, Kocher (col. 13, lines 20-67) discloses cryptographic operations should normally be checked to ensure that incorrect computations do not compromise keys or enable other attacks. Kocher discloses a technique of performing cryptographic operations twice, ideally using two independent processors and/or software implementations, with a comparison operation performed at the end to verify that both produce identical results. Kocher discloses, in situations where security is more important than reliability, the device may disable itself or self-destruct (e.g., by deleting internal keys) if the comparison of two cryptographic operations fails. In contrast, applicant discloses the stopping of a first cryptographic algorithm if a test ciphertext is generated for a test plaintext that corresponds to an apoptosis key. Kocher does not disclose or suggest the checking using a test plaintext, a test ciphertext, and an apoptosis key, as has been claimed.

Tschudin discloses a need for a self-destruction mechanism inside a distributed mobile service (abstract). Tschudin discloses the execution of a self-destruction routine that depends on "environmental data" as requested by a read() instruction and provides an example of apoptosis in response to the decryption, via a key, of code encrypted at an originator's site (section 3.1) and then processed at the executing site. Tschudin does not disclose or suggest the checking using a test plaintext, a test ciphertext, and an apoptosis key, as has been claimed.

Although Kocher and Tschudin are both concerned with cryptographic techniques, their disclosed approaches are starkly different. Kocher checks internally for security compromises in a smartcard environment (e.g., checking for discrepancies between two test results) while Tschudin is vigilant for a kill message to arrive from an external source in a distributed mobile service environment. Kocher discloses multiple cryptographic operations using encryptors that yield results that are later compared whereas Tschudin checks for and decrypts an encrypted kill message that leads to termination of distributed services. Kocher also does not disclose a decryptor that has been relied upon by Tschudin to check for an apoptosis message. Accordingly, Kocher does not readily lend itself to modification by Tschudin.

The Patent Office asserted (page 6, lines 1-7, of the Office Action mailed June 21, 2005) "Kocher et al. do not expressly disclose including at least one apoptosis key K_i. Kocher et al. teach self-destructing keys. However, Tschudin teaches the concept of "apoptosis" related to distributed services and computer security (sections 3-5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use an "apoptosis key". One of ordinary skill in the art would have been motivated to perform such a modification to control the execution of services (Tschudin, sections 4-5)."

Neither Kocher nor Tschudin disclose or suggest an apoptosis key, as claimed, or the claimed technique which determines the existence of an apoptosis key, considered a compromise situation, when a test plaintext generates a corresponding test ciphertext under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i . Thus, claims 1-13 are not made obvious by Kocher and Tschudin, either alone or in combination.

The Patent Office asserted (page 8, lines 1-8, of the Office Action mailed June 21, 2005) "Regarding claim 7, the combination of Kocher et al. and Tschudin does not expressly disclose publishing said at least one test plaintext P_i and for each test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i. However, Examiner takes Official Notice that publishing information was conventional and well known at the time the invention was made. Furthermore, Kocher et al. stores plaintext and ciphertext prior to comparing them. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to publish this information since Examiner takes Official Notice that it was conventional and well known."

Applicant challenges the Patent Office on the taking of Official Notice and requests a teaching applicable to Kocher and Tschudin (or other asserted reference or combination of references) that allegedly discloses or makes obvious claim 7 including limitations from base claim 5 and specifically requests a teaching for the limitation of "the step of publishing said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i."

The Patent Office rejected claims 2, 4, 6, 9, and 12 under 35 U.S.C. 103(a) as being unpatentable over Kocher et al. and Tschudin as applied to claims 1, 5, 8, and 11 above and further in view of Esserman et al. (US Patent Number 5,144,664).

Kocher discloses redundancy to determine security compromises through encryption and relates to a smartcard environment. Tschudin discloses checking for a kill signal through decryption and relates to distributed mobile services. Esserman discloses switching encryptors having different security algorithms and relates to broadcasting TV signals. Even if Kocher were combinable with Esserman, one of ordinary skill would not look to Tschudin as Kocher is concerned with encryption and the methodology of Tschudin entails decryption.

Furthermore, none of the references Kocher, Tschudin, or Esserman disclose or suggest an apoptosis key, as claimed, or the claimed technique which determines the existence of an apoptosis key, considered a compromise situation, when a test plaintext generates a corresponding test ciphertext under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i . Thus, claims 2, 4, 6, 9, and 12 are not made obvious by Kocher, Tschudin, or Esserman, alone or in combination.

The Examiner is respectfully requested to reconsider and remove the rejections of the claims under 35 U.S.C. 103(a) of 1, 3, 5, 7, 8, 10, 11, and 13 based on Kocher, U.S. Patent No. 6,327,661, in view of Tschudin (NPL Apoptosis – the Programmed Death of Distributed Services) and the claims 2, 4, 6, 9, and 12 based on Kocher, U.S. Patent No. 6,327,661, in view of Tschudin (NPL Apoptosis – the Programmed Death of Distributed Services) and further in view of Esserman, US Patent Number 5,144,664, and to allow all of the pending claims 1-13 as now presented for examination. An early notification of the allowability of claims 1-13 is earnestly solicited.

Respectfully submitted:

Walter J. Malinowski November 4, 2005

Walter J. Malinowski Date

Reg. No.: 43,423

Customer No.: 29683

HARRINGTON & SMITH, LLP
4 Research Drive
Shelton, CT 06484-6212

Telephone: (203)925-9400, extension 19
Facsimile: (203)944-0245
email: wmalinowski@hspatent.com

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

11/4/2005 Elaine F. Mian

Date Name of Person Making Deposit